UNITED STATES DEPARTMENT OF COMMERCE
National Oceanic and Atmospheric Administration
NATIONAL ENVIRONMENTAL SATELLITE, DATA AND INFORMATION SERVICE
Silver Spring, Maryland 20910

FEB 11 2009

MEMORANDUM FOR: Distribution

FROM: Zachary G. Goldstein
Chief Information Officer
NOAA Satellite and Information Service

SUBJECT: Practices for Securing Open-source Project for a Network Data Access Protocol Server Software on NESDIS Information Systems, v2

Attached is a revision to the NESDIS guideline that delineates mandatory and recommended information security practices to be followed when installing Open-source Project for a Network Data Access Protocol (OPeNDAP) Server4 software on a NESDIS information system. This revision clarifies the requirements for OpeNDAP server registration and clarifies the procedures for treatment of the OpeNDAP server as part of a parent system.

These practices for securing OpeNDAP servers are effective upon issuance for all new instances of OpeNDAP server registrations and configurations. NESDIS has not changed its policy requiring migration to version 4 or higher no later than September 30, 2009, and requiring all new instances of OPeNDAP implementation within NESDIS during FY 2009 to be version 4 or higher and to comply with this guideline for securing the application.

This guideline is effective immediately. If you have any questions, please contact Brennan Hay at Brennan.Hay@noaa.gov or phone (240) 676-3987.

Enclosure

Practices for Securing Open-source Project for a Network Data Access Protocol (OPeNDAP) Server4 (Hyrax) Software

NESDIS Office of the CIO
v2, February 11, 2009

This guideline provides instructions for mitigating known risks in OPeNDAP Server4 (Hyrax) software. Some of the following practices are mandatory and others recommended. If you cannot comply for a compelling reason, you are required to submit a request for waiver and provide the justification for it in your server registration.

Mandatory Practices:

1) Register the OPeNDAP server with NOAA.
   a. The server shall be registered with NOAA-opendap@noaa.gov.
   b. The N-CIRT, seconded by NESDIS OCIO, has right of first refusal to validate any OPeNDAP configurations before the system goes into production.
   c. A point of contact and alternate shall be identified with NOAA email address, phone number and NOAA system ID number.
   d. A network map shall be provided showing IP addresses, open ports and protocols from network entry to the OPeNDAP server, to include all N-Tier infrastructure.
   e. The communication via email with the above address shall be encrypted using the public key of the NOAA-opendap@noaa.gov email address.

2) Document the OPeNDAP server as a component of a parent general support system or major application for purposes of Certification and Accreditation (C&A).
   a. The C&A boundary for the system within which each OPeNDAP server resides (i.e., the parent system environment) shall include the OPeNDAP server as a component or subsystem of the parent system.
   b. The system owner shall assess the risks associated with the addition of the server in accordance with existing configuration change management procedures, and the component/subsystem shall be included in annual continuous monitoring, quarterly vulnerability scanning, and periodic C&A of the parent system.

3) Characteristics of OPeNDAP Server host operating systems
   a. The OPeNDAP host operating system shall not be placed on any Windows-based platform, not including Windows servers hosting Linux via a type 2 hypervisor.
   b. The server shall be placed on a hardened platform using the most current Defense Information Systems Agency Security Technical Implementation Guide (DISA STIG) for Linux, or equivalent.
   c. Any OPeNDAP server shall have OPeNDAP binaries that have the apparent disk root directory changed for the current running process and its children (i.e., Linux Chroot environment).
   d. Any OPeNDAP server shall employ Security Enhanced Linux Role-Based Access Control, or equivalent.
   e. Any operating system upon which the OPeNDAP file system is used shall have a file system integrity monitor, e.g., Tripwire, or an open-source equivalent monitor that provides the functions of change identification, daily reading of log files and automated reporting. Encrypted e-mail is acceptable.

f. All software developed for OPeNDAP, or as part of an OPeNDAP N-tier infrastructure, shall be evaluated by system owner staff for vulnerabilities using static analysis and any vulnerabilities discovered shall be addressed prior to deployment.
g. All software developed for OPeNDAP, or as part of an OPeNDAP N-tier infrastructure, shall be managed via a source control and configuration management process.
h. A staging infrastructure shall be created for security analysis and testing of OPeNDAP prior to the software moving to a production environment. The staging infrastructure shall be protected from public access, and any access to users outside of the system boundary shall be via Virtual Private Network, at a minimum.

4) Applications interfacing with OPeNDAP
Note: the following is specific to N-Tier infrastructure only and is not intended to include non-persistent client connections.
   a. Any server operating system with which an OPeNDAP server interfaces shall require the same protections listed above for OPeNDAP host operating systems.
   b. Any HTTP daemon with which OPeNDAP interfaces shall be hardened using the applicable DISA Web server STIG, or equivalent.
      i. HTTP daemons shall use Mod Security or equivalents.
   c. Any Database with which OPeNDAP interfaces shall be hardened using the applicable DISA Database STIG, or equivalent.
      i. Database servers shall use a database firewall.

5) Network requirements for OPeNDAP
   a. The particular subnet shall be access controlled using the subsystem firewall.
   b. If the OPeNDAP network connects to another network, a firewall shall exist between the connections. The firewall shall be configured to the minimum required protocols and ports for functionality for Moderate and High systems. The firewall log shall be reviewed regularly for systems of Moderate and High impact It is recommended that the frequency of reviews be daily, and be performed by System Owner staff.
   c. For Moderate and High impact systems, this subnet shall be monitored by a network intrusion detection system or intrusion protection system that is operational, maintained, and for which logs are reviewed daily.

Recommended Practices:

1) Network requirements for OPeNDAP
   a. Any OPeNDAP server should reside on a solitary subnet upon which only members of the OPeNDAP subsystem reside.
   b. All infrastructures on this subnet should be hardened using the appropriate DISA STIG, e.g., Network for routers and switches, or equivalents.
   c. Upon this subnet, a network intrusion detection system or intrusion protection system should be operational, maintained, and for which logs are reviewed daily.

Record of Changes

Effective Date	Change	Authorized by/date
09/30/2008	Issuance of version 1.	Zachary Goldstein 10/21/2008
02/11/2009	Issuance of version 2. • Moved practice 2.c. into practice 1. • Clarified the steps for registering an OpeNDAP server in mandatory practice 1. • Clarified treatment of OpeNDAP server as a component of a parent system for purposes of C&A in mandatory practice 2.	Zachary Goldstein 02/11/2009